# Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences

# Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences

Rick Wash, Emilee Rader, Kami Vaniea, Michelle Rizor
Department of Media and Information
Michigan State University
{wash,emilee,vaniea,rizormic}@msu.edu

## ABSTRACT

When security updates are not installed, or installed slowly, end users are at an increased risk for harm. To improve security, software designers have endeavored to remove the user from the software update loop. However, user involvement in software updates remains necessary; not all updates are wanted, and required reboots can negatively impact users. We used a multi-method approach to collect interview, survey, and computer log data from 37 Windows 7 users. We compared what the users think is happening on their computers (interview and survey data), what users want to happen on their computer (interview and survey data), and what was actually going on (log data). We found that 28 out of our 37 participants had a misunderstanding about what was happening on their computer, and that over half of the participants could not execute their intentions for computer management.

## 1. INTRODUCTION

Home computer software is rarely released problem-free; most companies release a number of *software updates* to fix bugs in the software and add in new features. Microsoft alone released over 300 distinct software updates in the first three months of 2013. *Security* updates are particularly important because they are one of the primary mechanisms for protecting home computers from malicious software that leverages known vulnerabilities. The majority of computer compromises result from vulnerabilities for which a security update is available but has not yet been installed [16, 19]. Timely installation of security updates can protect users from the most common attacks [19].

Since installing security updates is so important for computer safety, many software companies have worked to find ways to improve end-user compliance and increase the number of fully updated systems. For example, each successive version of Microsoft Windows has had additional features to automate the installation of software updates with less human involvement [10]. Current software updates (and Microsoft Windows Updates in particular) have largely removed the need for human decisions. They default to automatically downloading and installing updates in the background, and forcing users to reboot (if needed).


*Symposium on Usable Privacy and Security (SOUPS)* 2014, July 9–11, 2014, Menlo Park, CA.

However, not all security technologies can completely remove the human from the decision-making process [1]. Cranor assembled a useful framework for reasoning about when it is advisable to keep a 'human in the loop' [5]. This framework is relevant to software updates because updates cannot be installed completely without user intervention for three reasons: 1) occasionally, an update will introduce a new bug into the system, and users will want to postpone installing that update, 2) an update may introduce or remove features which impact user activities causing users to want to avoid installing the update, and 3) many updates require rebooting the computer to install, which is highly disruptive of user activities. Therefore, users need to be kept informed and given options during the update process. Software update systems have tried to accomodate users by finding an appropriate balance between forcing users to install updates to improve security, and giving them appropriate choices.

We conducted a multi-method user study to better understand how people make decisions about software updates that are so crucial to security. With each subject, we conducted semi-structured interviews to understand how the subject views software updates, had him or her take a survey to provide more structured opinions, and collected log data about update installation from his or her computer. In this paper, we focus primarily on subjects' decisions and behavior for Microsoft Windows updates. We find that over half of our subjects were not aware of what their computer's software update settings were or when the software updates were being installed. The majority of users' computers behaved in a way contrary to the user's intentions. However, many of these computers were also more secure than the user intended. This means that improving usability of software updates might not lead to improved security, which has interesting implications for the design of software update systems.

## 2. INTEGRATING HUMANS INTO SECURITY

Security failures are often seen as a human problem rather than a technological one. For example, West [24] wrote, "The most elegant and intuitively designed interface does not improve security if users ignore warnings, choose poor settings, or unintentionally subvert corporate policies."

In the workplace, computer and information security is the joint responsibility of end users and system administrators, but end users are often seen as "inherently insecure" [1, 11]. With the rise of discretionary computer usage and "bring your own device," end users bear more of the responsibility for the security of their many devices in and out of the workplace. Such users are their own system administrators, whether they know it or not, and how to best support them is the subject of much research.

Users are perceived as the weak link for several reasons:

- The expectations placed on end users with respect to managing the security of their computers are unrealistic; users cannot be expected to think like system administrators [2]
- Security only becomes apparent to end users when something has already gone wrong [27]
- Security is not users' first priority, and given a choice, they will choose the insecure option if it gets them closer to their goals [8]
- When users make mistakes, it makes the job of system administrators that much harder [8]

System designers frequently attempt to either nudge [20] or force users into making secure decisions. The designer might try to make security the user's top priority by creating mechanisms that prevent them from completing any action until the security aspects have been taken care of. The system might make the security-related actions so easy and unobtrusive that they can do whatever is necessary as part of their normal workflow or primary task (path of least resistance). Or, it might remove all responsibility and ability to act from the user by completely automating the security aspects of the system, so users cannot make the wrong choice [26].

However, it isn't feasible to completely automate security. Human capabilities are frequently necessary for the task at hand [22]. A "default" level of security is not appropriate for all users in all situations [9]. And automatic security cannot be used when configuration decisions must be made, or when automation is too "restrictive, inconvenient, expensive, or slow" [9]. Cranor [5] advocates that system designers should explicitly design for both automation and user responsibility for security by identifying which security aspects of the system cannot be automated and are likely to fail due to user intervention. System designers should provide better support to the users in those circumstances.

Software designers need to be aware that there is a tradeoff between visibility and intrusiveness. In circumstances when the user must remain "in the loop", communication between the system and the user is crucial, and it is the role of the software designer responsible for making sure the software is secure to figure out where this communication must take place [5]. Relegating security to "Advanced" tabs and burying it in menus is one way to (intentionally or unintentionally) ensure that the user retains the defaults. [9]

How that communication might best be accomplished is the subject of much usable security research. One of the core values of usability is "walk up and use" interfaces that do not require special learning or expertise; however, this approach may result in prioritizing the usability aspects of the system over the security aspects, because security may be more complicated than a "walk up and use" interface can communicate [12]. Recommendations to improve the usability of the communication between the system and the user are often assumed to also improve security, because users will be more involved, but this is not always the case.

To further complicate matters, end users often delegate the responsibility for the security of their systems, to technology, other people, organizations, or institutions [7]. Delegating responsibility to technology—to the system itself—is like 'set it and forget it' security: do it once, and never have think about it again. Once this has taken place, security becomes invisible, and is not often revisited. This means that the system keeps going with the past settings indefinitely. Policies like this are too rigid, because an invisible policy can't adapt to users' changing needs and circumstances [8].

Software updates are a particularly interesting case for studying how to include humans in security systems. From a security perspective, quickly installing security updates is the correct behavior, and can often be safely initiated without user intervention. However, many updates require that the computer reboot to complete installation, necessitating human involvement, and making the automated update process visible to users who may not understand why it is necessary [21].

# 3. SOFTWARE UPDATES IMPROVE SECURITY

Updating software is an important part of keeping a computer secure, and keeping all software up-to-date will protect a user against the most common security exploits. Symantec has data showing that the majority of computers are compromised using vulnerabilities where an update is available, but has not yet been applied [19]. The majority of web exploits use the top twenty vulnerabilities, all of which have available updates [19]. Likewise, Microsoft observes that all of the vulnerabilities exploited by the most popular exploit kit have available updates [16].

It is important to update software as soon as possible after a security update is released. Updates correcting security vulnerabilities are released an average of 1.2 months after an exploit for the vulnerability seen in the wild [15]. However, exploits released before a vulnerability becomes public knowledge (zero-day vulnerabilities) are used to attack a relatively small number of computer systems. Once a zero-day vulnerability becomes public knowledge the number of exploits using it increases 183–85,000 times and the number of attacks increases 2–100,000 times [3]. Likely for this reason, 60% of Microsoft's vulnerabilities are made public knowledge the same day as the update correcting the vulnerability is released [15], enabling users to protect themselves before exploits become readily available. For these and other security reasons, the faster the user updates their system the less likely they will be vulnerable to new attacks.

While updating quickly is good for security, all updates cannot be completely automated because they impact end users' workflows [21]. Many software updates include new, unwanted features. Some software updates introduce new bugs or incompatibilities. Rebooting interrupts users from their work. And many users prefer to "not fix what ain't broken."

There has been limited investigation into what motivates users to update or not update software on their computer. LaRose et al. surveyed undergraduate students about their online safety behaviors and beliefs. They found that people who feel like online safety is their personal responsibility are more likely to want to perform safe online behaviors [13, 14]. They also found that coping efficacy beliefs were correlated with intention to perform software updates [13]. These studies are based on self-report data, and are unable to examine whether subjects actually undertake their stated behaviors.

## 3.1 Windows Update

In this paper, we focus on Windows Update, a software update service provided for free by Microsoft. It began as a website that Windows 95 users had to visit to find out whether operating system updates were available. A new "Critical Update Installation Tool", introduced with Windows 98, included automatic checking for updates, and it also notified users about critical updates which they had to then manually retrieve and install. In 2000, Windows ME shipped with "Automatic Updates", a tool that could automatically download and optionally install software updates. Automatic installation of updates became the default with Windows XP SP2, and Windows Vista began automatically installing both updates categorized as "important" (including 'security' and 'critical' updates

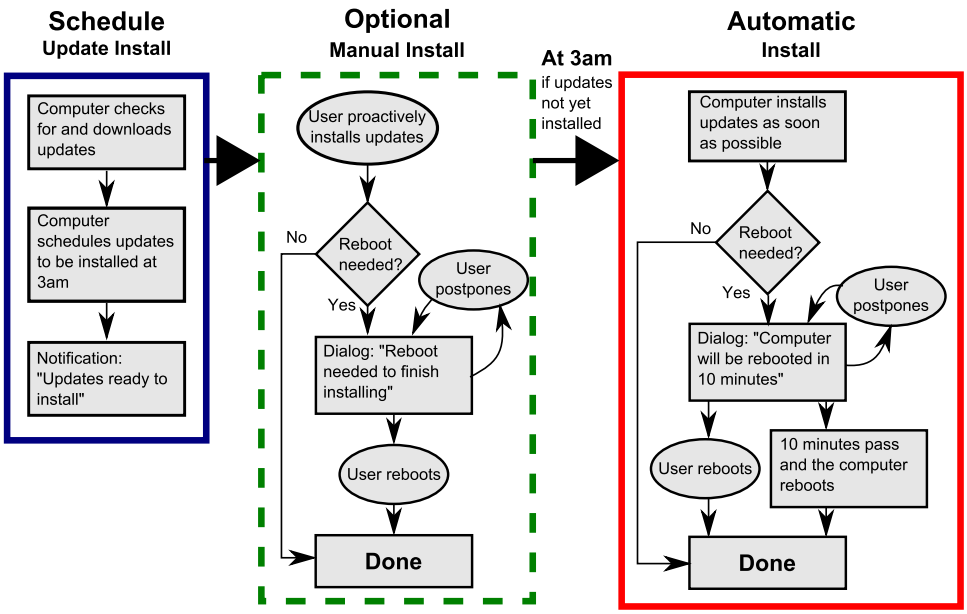



**Figure 1: The Windows Update process. Ovals represent user actions, diamonds decisions, and rectangles computer behavior. This diagram was created based on prior update work by Gkantsidis et al., and experimentation using a Virtual Machine with Microsoft Windows 7 Service Pack 1 installed.**

as well as reliability improvements), and also "recommended" updates [25].

The result of this evolution, the Windows Update software used in Windows 7, demonstrates the compromise Microsoft software designers made between automating the update process for the safety of users and giving users responsibility for their computer use. As shown in Figure 1, by default each update in Windows Update goes through three stages: an install scheduling, a time for manual install, and an automatic installation.

**Stage 1**: (left blue box) The computer automatically checks for updates, downloads them, schedules them to be installed at 3am the next morning, and then notifies the user that updates are available to be installed. The notification appears temporarily in the bottom right of the screen, and a gold shield is added to the "Shut down" button on the start menu.

**Stage 2**: (green middle box) The computer waits silently for the user to manually initiate the install process. This gives the user the opportunity to take responsibility for their updates. Users may manually install updates by opening the Windows Update program and selecting "Install updates." If a reboot is needed, the user is notified by a dialog with a postpone option. However, the dialog only reminds the user, it does not compel a reboot.

**Stage 3**: (red right box) The computer starts installing updates automatically at 3am or the first time the computer is turned on after 3am. If any update requires a reboot the computer presents the user with a dialog warning that the reboot will happen in 10 minutes. The dialog countdown timer has options to "Reboot now" or "Postpone"; the user cannot escape the countdown completely. If the user does nothing, the computer will immediately reboot. However, if the user chooses to intervene during the 10 minute interval, they can "Restart now" which causes an immediate reboot of the system, or "Postpone" for an additional 10 minutes, 1 hour, or 4 hours. This stage automates security decisions, removing the human from the loop.

The design of Windows Update is a compromise between fully automating updates and giving users full responsibility for updates, and it has been successful at increasing security. After the release of Windows XP SP2, Gkantsidis et al. observed that only 5% of SP1 users had fully updated computers, but 90% of SP2 users had fully updated computers. They also observed that 80% of SP2 users downloaded the latest update within two days of release [10]. In 2011, 66% of Windows users (all versions) were completely up-to-date, and 84% had at least one of the three most recent updates [16].

# 4. METHODS

Software updates are an instance where security system designers have mostly, but not completely, removed humans from security decision-making. To better understand user decision-making about software updates, we undertook a multi-method study that included semi-structured interviews, an online survey, and log-data analysis. This allowed us to measure both users' beliefs and impressions about what their computers were doing, and what their computers were actually doing.

## 4.1 Participants and Protocol

To study software updates, we wanted a population that doesn't have formal security or computer administration training, but still thinks enough about issues around updates that they have relatively well-formed opinions. We chose to study graduate students at a large research university in the Midwest of the United States. Graduate students are a group of computer users who are mostly non-technical, are responsible for maintaining their own computers, and depend on their computers for their work.

We sent an email through the University Registrar to a random sample of 1000 graduate students, excluding Math and Engineering students, asking for volunteers to participate in the study. Ninety-five people took a screening survey to ensure that they were Windows 7 users (so we could collect log data) and did not have any formal training in computer management, IT, or system administration. For this study, we chose to go deep into a single system's

updates, and chose the most popular, and most commonly exploited end-user system (Windows) to focus on. Thirty-seven people who were eligible came to our lab to participate, and brought their laptop running Windows 7 with them. Three of these subjects were Mac users running Windows in a virtual machine. Participants ranged in age from 21 to 57 with an average age of 31; Seventeen were male, and twenty were female. These demographics approximately match those of the larger graduate student population.

After informed consent, the study consisted of three parts: a brief survey, Windows log data collection, and a semi-structured interview. While one member of the research team administered the survey and interview, another member used a custom Powershell script to collect setting and log data on the subject's laptop. Subjects were given the option of observing the data collection. This study was approved by our university's IRB.

## 4.2 Three Types of Data

We collected three different datasets from each participant: a set of survey responses, log data from their Windows 7 laptop, and a transcribed, semi-structured interview. We began by analyzing each type of data separately. Then, using an ID number and pseudonym assigned to each subject, we re-combined the three data sources to compare subject responses and behavior across data sources. This analysis structure ensured that we accurately understood the meaning of each separate type of data before comparing attitude, recall, and behavior across data sources.

### *4.2.1 Semi-Structured Interviews*

System designers have made most software updates highly automated and relatively invisible to end users. Users don't spend much time thinking about software updates. This poses a challenge for conducting interviews: how can we get subjects to talk about past experiences and reveal how they think about updates? And how can we avoid having subjects think about updates too deeply during the interview – and change their opinions, which would lead to invalid data?

After a series of pilot tests, we decided to use three interviewing techniques: free-listing, hypothetical scenarios, and recollection of specific past instances.

We began by asking participants to complete a *free-listing activity* [4]: write down as many examples as came to mind for the prompt, "things that can happen if the software on your computer is too old or out of date". We then read each example and asked the participant to discuss his or her response further. Free-listing allows us to explore the semantic domain of updates; that is, it helps the subject to think through and explain the range of activities and concerns that are relevant to a discussion of software updates. The use of a non-specific prompt, reading items back to the subject, and using the items as semantic cues to discuss past instances help subjects to fully explore the topic of software updates [4].

Next, we presented subjects with a series of five *hypothetical scenarios* paired with probing questions; we wanted the participant to do most of the talking so that we could uncover their attitudes, beliefs, and mental models about updates. The scenarios involved being prompted to restart an internet browser mid-task, seeing that a large number of urgent Windows updates were available, reading a news article about a virus, a software program that costs money to update, and a slow computer with lots of warnings. Hypothetical scenarios are effective methods of learning how subjects conceptualize their decisions relate to software updates [23].

Finally, throughout the interview, we regularly asked subjects to *recall specific past instances* of software update decisions. By asking to recall specific instances, subjects provide more details and are better able to recall information that influenced their decision-making at the time. Recalling specific instances provides data that is more likely to represent broad decision-making patterns than asking subjects to describe general patterns of past behavior [18].

**Analysis**: After transcribing and anonymizing the interviews, we performed a bottom-up, inductive coding. We started with an initial list of themes identified by the research team, and expanded the codes as each of us separately read through transcripts. During this period, members of the team met frequently to discuss and revise the codes. Themes identified include "negative update experiences", "attitudes toward delaying updates", and "why updates are important."

As we created each code, we examined other subjects to check for representativeness and identify which traits were common across subjects. We also explicitly looked for negative cases: cases that share most of the pattern but are explicitly missing one or two key pieces.

When coding was complete, we summarized the data into a matrix that displayed themes by participant [17]. This matrix allowed us to understand each individual's perspective on updates by reading down the column that summarizes their responses. We then compared the summary data matrix to original interviews to verify the correctness of each summary, check for the meaning of outliers, verify surprises, specifically look for evidence for negative cases, and try to prevent researcher confirmation bias in our data. [18]. This process provides confidence that our summaries are valid representations of participant views as expressed in the interviews.

### *4.2.2 Survey*

We used an in-lab computer survey to ask structured, closed-ended questions. A survey allowed us to ensure that all participants were asked the same set of factual and opinion-based questions in a consistent, comparable manner. In addition to background information such as subject demographics, computer skills, and installed software, we also asked subjects for their current understanding of the state of software updates on their computer. This includes whether automatic updates were enabled and whether updates were usually installed manually or automatically. Questions were written following the guidance of Dillman [6] and were pretested to ensure subjects understood the questions the same way the researchers did.

**Analysis**: We generated descriptive statistics for each subject, as well as extracting the specific questions about the user's knowledge of current state of the automatic updates setting, their belief about whether updates are installed manually or automatically, and their belief about the timing of install. The full survey instrument is available in the Appendix.

### *4.2.3 Windows Logs*

The Windows operating system, along with many Windows services, records information about system events in log files which contain detailed records of system and user behavior. Our Powershell script collected the current Windows Update settings, which allowed us to determine whether updates were turned off, set to notify the user before download, or set to install automatically without user intervention (default behavior). The script did not collect any personally identifiable information.

We also collected a list of installed updates from the Windows Update API, and a copy of all Windows Update log files which provided detailed event information from the last several months of use. This allowed us to calculate the time between when an update had been downloaded and when it was installed, which is important because this is the part of the update process that the user has

the most control over—i.e., when the update is installed and when the computer reboots to finish installing an update (if necessary). One limitation of this method is that the detailed logs represented between 1 and 17 months (average of 6) of usage data depending on how often the participant had been using the machine.

**Analysis:** We first looked at each update separately. We limited our log analysis to updates which were associated with a Microsoft Knowledge Base (KB) number, which allowed us to link update events across log files. We marked the update as proactively installed by the user if it was installed before 3am[1] the morning following the update's download. We marked it as automatically installed by Windows Update if it was installed after 3am. Then we aggregated all updates for a user: did the user always install proactively (100%), usually (> 50%) install proactively, usually automatic install, or always automatic install?

## 4.3 Combining Data for Analysis

In order to compare user attitudes, user beliefs, and user behavior, we constructed a data matrix that combined data from all three sources of information [17]. For each subject, we created entries on three topics: general updates, the automatic updates setting, and the timing of update installs. For each of these topics, we included a row of data from each of the three data sources: the subject's attitude and understanding of the topic summarized from the interviews, the subjects current beliefs from the survey, and the subject's past behavior summarized from the log data.

After creating the combined data matrix, we again examined our data to ensure validity [18]. All members of the research team participated in looking for patterns across subjects, checking for negative cases, verifying summaries with original source data, and including footnotes and caveats for our summaries.

For each of the three topics, this data matrix allowed us to directly compare a subject's understanding, the subject's belief, and the subject's behavior on their computer. In checking through this data matrix, however, we noticed that subjects' understanding and beliefs were not straightforward. Rather, each subject's understanding and beliefs could be separated into two: the subject's understanding of what his or her computer is currently doing, and the subject's intention for what he or she would like the computer to be doing. Therefore, we split these understanding rows in two, and verified each piece with the source data.

# 5. FINDINGS

We used our interview data and our survey data to characterize two things: what the user thought the computer was doing, and what the user wanted the computer to do. We then compared these two perceptions with the log data from that user's computer to determine if they matched. That is, we compared user's stated *understanding* of what their computer was doing with log data and settings that indicated what the computer actually did, to see whether users understood what was happening on their computer. Then we compared each user's stated *intentions* — what they wanted their computer to be doing — to the log data and settings to determine whether they were actually able to make the computer do what they wanted.

## 5.1 Understanding Software Updates

Many of our subjects misunderstood what their computers were doing regarding software updates. Twenty-eight of the 37 subjects (78%) had at least one inconsistency between what the subject thought their computer was doing and what the log data indicated it was doing. There are two topics that subjects had misunderstandings about: the Windows Update setting about whether to install updates automatically, and how quickly updates were installed.

| *Consistent* | | *Inconsistent* | |
|---|---|---|---|
| Changed Setting | 4 | On, but thinks Off | 4 |
| Default Setting | 8 | Off, but thinks On | 2 |
| | | Download but not Install | 5 |
| | | Notify, but not Download | 14 |
| Total | 12 | Total | 25 |

**Table 1: Misunderstandings of Automatic Updates (Number of Subjects)**

### *Automatic Updates Setting.*

Automatic update settings were a prevalent source of misunderstanding for our subjects. There are four possible settings in Windows Update: 1) *On*, the default setting where Windows automatically downloads and installs updates according to the process described in Section 3.1 (31 participants had this setting), 2) *Download* available updates but do not install them (0 participants), 3) *Notify* the user when updates are available, but do not automatically download or install them (4 participants), and 4) *Off*, where Windows Update must be manually run for anything to happen (2 participants).

Among our 37 subjects, 25 had some form of inconsistency between what they stated they thought their computer's auto-update setting was, and the recorded settings on the computer (See Table 1). Of these, five subjects were close to correct: they thought that their computer automatically *downloaded* updates and prompted them to install. While this is true, their actual setting automatically installs the downloaded updates at 3am if the user hasn't already installed them; these five subjects frequently installed their updates proactively so rarely encountered the 3am automatic install.

This leaves 20 subjects who had an inconsistency in their understanding of their auto-update setting. Four subjects believed that their auto-updates had been turned off, when in reality they had the default, secure setting of automatically installing updates. Two subjects believed the opposite; they thought they had auto-updates turned on, but auto-updates had been disabled on their computer[2]. The remaining 14 subjects expressed a belief that automatic updates only notify them about available updates but do not install them. However, these 14 subjects all had the default setting of automatically installing updates. For example, Justin[3] told us "I mean it usually prompts me when there is an update to be installed, but I don't know if that means auto-update or not." His survey answers also indicated that he thought that Windows notified him, but did not install updates.

As a comparison case, 12 subjects were completely consistent in their understanding of auto-updates. Eight had the default setting, and correctly understood that setting as automatically downloading and installing updates. Rachel said, " I guess my current belief is that the operating system doesn't give you a choice about updating things, it just does it for you." And four subjects had intentionally changed the setting to *Notify Before Download* (i.e., the computer notifies the user that new updates are available but does not down-

[1] One user had a scheduled install time setting of 4am, all other users had the default of 3am, for simplicity we always refer to this time using the default of 3am or "overnight".

[2] One of these subjects may be running a third-party updating system designed for pirated Windows systems.

[3] All subject names have been anonymized.

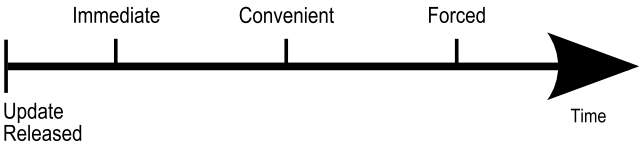



**Figure 2: Perceived Times When Updates Can Be Installed**

load or install them), and also correctly understood their change.

In our sample of non-technical computer users, six subjects' computers did not have the default auto-updates setting, *Scheduled Install*, in which software updates are automated as much as possible. Two of these subjects didn't understand the setting and thought they were still on. However, the remaining four subjects correctly understood that their computers would not automatically install updates. An additional 14 subjects, who had the default setting of *Scheduled Install*, believed that they were only notified about updates and that no updates were installed automatically. These findings indicate that many misunderstandings exist regarding whether users are updating Windows, and that sometimes these misunderstandings mean that updates are not installed.

### *Timing of Update Installation.*

The timing of updates is another source of inconsistency between subjects' stated intention and log data. Common security advice is that software updates, and particularly security updates, should be installed as quickly as possible to protect against in-the-wild exploits and zero-day vulnerabilities [19]. However, installing software updates usually interrupts what the user is doing on their computer, and often requires a severely disruptive reboot [21].

In our log data analysis, we characterized each update as either *proactive* or *automatic* depending on if the user proactively installed the update, or if Windows automatically installed the update. Each subject, then, made a series of choices that either resulted in the subject installing most of their updates proactively, or mostly allowing Windows to automatically install.

However, subject understanding of update timing doesn't exactly match this characterization. Instead, we found three timing categories for when updates might be installed (See Figure 2). The fastest possible update installation happens when a user is notified about an available update, and interrupts what they are doing to *immediately* and manually install the update. An intermediate timing occurs when a user is notified about an update, but doesn't interrupt their work to install it immediately. Instead, they wait until a *convenient* time to manually install the update. Both these categories involve manual installation, though some users may not find convenient times and end up with Windows automatically installing some updates. Finally, the slowest timing that actually results in the update being installed corresponds with the *forced* timing, and occurs when the user waits too long and the computer automatically installs the update and reboots the computer.

This difference in technical coding and user understanding poses an analysis challenge: when a subject indicates that they install their updates "when convenient," how do we characterize whether their behavior is consistent with their understanding? To address this, we first looked at the logs for whether most of an individual subject's updates were automatic or manually installed. If updates were mostly automatic, then that is a clear disconnect from the subject's stated understanding of installing when convenient; since the automatic install happens as pre-specified times, it is unlikely that that is happening "when convenient."

However, if the subject mostly installed updates manually, then this could be consistent with a desire for convenience (if they waited until it was convenient to install and reboot), or it could be inconsistent (if they interrupted themselves to install the updates). Since whether or not a subject was interrupted is entirely in the opinion of that subject, we looked to the survey data for guidance on how to categorize them. On the survey, we asked each subject how likely they would be to interrupt themselves to install Windows updates. Consistent with traditional interpretations of similar Likert scale survey questions [6], we took this question to represent the subject's memories of whether they were frequently interrupting their work to install updates. If they answered "Likely" or "Very Likely", then we took this as inconsistent with their stated desire for convenience. Any other answer was considered consistent.

| *Consistent* | | *Inconsistent* | |
|---|---|---|---|
| When Convenient | 8 | Want Convenience, but Automatic | 8 |
| | | Want Convenience, but Proactive | 6 |
| Wait till Forced | 6 | Thinks Delay, Installs Proactively | 2 |
| | | Wants Only AV updates | 2 |
| | | Turned Auto-updates Off | 1 |
| Total | 14 | Total | 19 |

**Table 2: Inconsistencies in Timing of Update (Number of Subjects). We excluded four subjects from the table due to insufficient information.**

**Results**: Nineteen of our 37 subjects expressed a desire about the timing of updates that was inconsistent with the log data on their computer. Of these, ten subjects installed updates more quickly than their stated intention, and nine subjects installed updates more slowly. (See Table 2 for counts.) Four subjects had insufficient interview data to accurately judge their desires.

Twenty-two subjects stated that they wanted to install updates manually at a convenient time; however, eight of them never actually got around to running the updates and the computer ended up automatically installing the update — which means the subjects installed updates slower than intended. Six subjects actually interrupted their work and installed the updates very quickly. On the diagram in Figure 2, all 22 of these subjects' stated intentions were to install in that middle range of timing — when convenient. Eight actually installed at that time; eight actually installed when forced (to the right), and six actually installed immediately (to the left).

Two subjects stated that they usually delay updates, particularly updates that require a restart. These subjects, however, usually installed updates very quickly according to the logs. Three subjects said they only do updates labeled "urgent"; two of them successfully installed all updates quickly, but one subject had auto-updates turned off and didn't install any updates.

When a subject has an inconsistency about when updates are being installed, this isn't a technical misunderstanding. Subjects aren't misunderstanding how the computer is working. Rather, they are misunderstanding their own behavior. Such a misunderstanding is important because it can form the basis for further decisions, such as "is my computer secure?" But since it is not a technical misunderstanding, greater education will not necessarily solve it.

### *Difficulty Understanding Updates.*

As indicated by the many inconsistencies mentioned above, many of our subjects misunderstood what was happening on their computers. In examining our interview data, we found two reasons they were having problems.

First, the computer wasn't very clear about what it is doing and

when it is doing it. Many subjects talked about how it was difficult to understand what was going on. Nicole, for example, could not tell whether she permitted her computer to automatically update or not:

> Actually I didn't know that I clicked yes for auto updating. It just popped up. So, that's why I know about the auto updating. And other stuff, I didn't know that I clicked yes for auto updating or something like that.

In the interview, she indicated that she thought it was important to install urgent and critical updates, and in the survey she indicated that she thought her updates were automatically installed. However, her computer actually had automatic updates turned off.

Second, even when our subjects tried to look at settings and dig deeper, they found most of the settings to be confusing and difficult to use. Matt said that he "[doesn't] even know where I'd go to do that." Will wanted to turn off automatic updates:

> But I know I played around with some of the settings on my computer so that it wouldn't automatically update everything. Because it would just slow down my computer to a crawl. And several computers that I've had, it makes it harder when you're trying to get a task done.

However, Will's computer still had the default setting and all updates released had been installed. Furthermore, most of his updates were automatic installs, rather than being installed manually.

Many of these misunderstandings stem from design choices that try to remove the need for humans to make decisions about software updates. Windows Update has automated as much as possible and moved many updates actions into background, invisible processes. That automation made it difficult for many of our subjects to understand what was happening on their computer at any time, and even whether updates were being installed at all. Additionally, to discourage users from changing settings, Windows Update makes it difficult for users to find the settings in the first place. So even if our subjects did want to change the settings, they couldn't figure out how. Removing the subjects' decision-making ability had the side effect of also making it difficult for them to learn about updates and understand what their computers were doing.

## 5.2 Intentions and Security

In addition to describing their current understanding, our subjects also described what they wanted to be doing about software updates. Did our subjects intend to put off updates because they felt like updates weren't important, or did they intend to install them immediately but ended up delaying indefinitely? Here, we describe whether these stated *intentions* match what was actually happening on the computer. Mismatches between intentions and behavior indicate usability problems, or what would change if we made software updates easier to understand and use.

For this analysis, we consider installing updates to be secure, and installing them sooner is more secure than waiting and installing them later. While users may have good reasons to choose to be less secure, we focus primarily on the security consequences of those choices.

Two subjects provided short answers during their interviews and did not clearly describe their intentions for what they wanted their computers to be doing. Therefore, these subjects were removed from this analysis of intentions.

| *Consistent* | | *Inconsistent* | |
|---|---|---|---|
| Notify but not Auto-Install | 3 | More Secure | 12 |
| Not urgent, so wait till Forced | 3 | Less Secure | 9 |
| Always install Immediately | 8 | | |
| Total | 14 | Total | 21 |

**Table 3: Whether Intentions are Consistent with Reality (Number of Subjects)**

### *When Intentions Don't Match Reality.*

Twenty one subjects had a disconnect between their stated intentions for installing software updates and what the log data indicated their computer was actually doing (Table 3).

For nine of these subjects, the computer ended up being less secure than the subject intended. Three subjects intended to install updates regularly and automatically, but actually had their automatic updates turned off (or to notify) and had almost no updates installed on their computer. The remaining six subjects all stated that they intended to proactively install updates as soon as it was convenient, but rarely actually got around to installing the updates until the computer automatically did so. This mismatch between intention and behavior led to the updates being installed, but left a larger window of vulnerability than the subject intended.

As an example, Dan talked about how he chose when to install updates:

> If I were doing something fun I would interrupt it, no problem. If I were just surfing the web, it's like, oh, whatever, I'll update my computer. But if I'm writing an email, if I'm working on a paper, if I'm working on a homework assignment, then that usually takes priority. If I can put it off for 15, 20 minutes, I'll just do that later then, 'cause when I'm in the zone studying, I don't wanna be interrupted with anything.

This is a typical representation of a "convenient" intention: he wanted to install updates, but didn't want to be interrupted. So he said he'd finish what he was doing and then install the updates. However, Dan's computer logs indicated that Windows Update automatically installed most updates; he rarely installed them manually. This means that his computer was vulnerable for the maximum amount of time that Windows Update allows.

Twelve subjects had a disconnect between their stated intentions and the log data that left their computer more secure than they had intended. Two of these users explicitly stated that they wanted to turn automatic updates off, but their computer still had the default setting of automatically downloading and installing updates. Another example is a subject who wanted to continuously delay updates, indefinitely, but had the default auto-update setting that automatically installed updates in a relatively timely fashion.

One subject from this group, James, expressed an intention to delay updates until a convenient time, but always ended up interrupting what he was doing to manually install updates. He described one instance that illustrated his intention to install when "convenient":

> What was I gonna do? I was working on homework for something and I was loading a video on my browser to watch while I ate food. It was buffering and loading, and I usually will take a meal break and watch a movie at the same time. And I realized if I restarted, then that would have to reload, the movie would have to reload

> all the way from the beginning. And I would lose that time because I was going to eat in 15 or 20 minutes and then I had to go somewhere, I had a class. So I decided, you know what, I'll just postpone.

However, according to James's computer logs, all of the updates on his computer were installed, and were installed manually in less than 24 hours after being downloaded. James actually interrupted his computer use at some point rather than postponing, and ended up with a smaller window of vulnerability than he would have if he had waited to install when convenient.

These disconnects are interesting when we look at what would happen if we improved the usability of software updates and did a better job of including the user in the loop. Nine of our subjects' computers would be more secure if they were able to execute on their intentions, while twelve would be less secure. The sample for this study is not representative, so we cannot claim that these 21 out of 37 subjects (59%) generalize to the larger population of computer users. However, our sample has a relatively large number of both people who would be more secure if usability improved, and a similar number who would be less secure if usability improved. We suspect that both groups are well-represented in the larger population.

### *When Intentions Match Reality.*

Fourteen of our subjects were able to successfully execute on their intentions: the log data from their computer was consistent with these subjects' stated intentions for software updates. However, these subjects had varying levels of security.

Eight subjects fell into the most secure category; these subjects all had the default setting that automatically downloads and installs updates. These subjects felt strongly that installing updates is important, and manually installed updates soon after they were notified that the updates were available. These subjects didn't wait for the computer to automatically install the update. By manually installing the update, they minimized the window of vulnerability.

Three subjects had a strong objection to the way that Windows compels the computer to reboot; these subjects felt rebooting seriously interrupted their work. These subjects changed their settings so that Windows notified them that updates were available, but did not download or install them. They manually downloaded and installed updates at a convenient time. Everyone in our study who had changed their auto-update setting to *Notify Before Download* or *Notify Before Install* fell into this group; people who change this setting seemed to understand that updates are important and still install them, but not as quickly.

Finally, three subjects didn't feel like updates were that important, and wanted to have the computer deal with the updates for them. They continually postponed updates until the computer automatically installed the updates, and rebooted their computer.

### *Would Better Usability Be More Secure?.*

Many people in the HCI community emphasize usability; if we make computers easy to walk up and use, then people will be able to accomplish more with them. When people form intentions about what they want their computer to do, but cannot execute on those intentions, HCI professionals naturally suspect a usability problem. Indeed, Windows Update seems to have a usability issue; 21 of our 37 subjects (approximately 59%) were not able to use the system the way they wanted to.

However, it isn't clear whether better usability would actually be an improvement in this case. Only 9 of 21 subjects whose behavior did not match their intentions were less secure than they wanted to be; these subjects would end up more secure if we were to improve usability. But for the remaining 13 subjects whose behavior did not match their intentions, the computer was more secure than it would be if usability were improved. These subjects wanted to be less secure, and poor usability was preventing them from executing on that intention.

Many of our subjects had misunderstandings about what their computer was doing with software updates. And many of our subjects had trouble executing on their intentions. One reasonable assumption is that the second statement — the difficulty in executing on intentions — is caused by the first. However, we don't believe this is the case. A couple of subjects completely understood what their computer was doing, but still could not execute on their intentions. For example, Rachel understood that the computer was installing updates, but felt like auto-updates were controlling her and forcing her to install them. And there were many subjects who didn't understand what their computer was doing, but ended up doing exactly what they wanted to. Brittany believed that her computer only notified her but didn't install updates; however, she wanted to control her updates and ended up installing almost all of her updates manually at convenient times. It seems that understanding is not necessary to be able to execute on security intentions.

## 6. DISCUSSION

Our subjects had a number of misunderstandings about what their computers were doing with respect to software updates. Also, our subjects frequently were not able to execute on their intentions about whether and when to install software updates. We speculate that these challenges may be the result of trying to remove the human from security decisions. We also observe that improving usability may actually backfire.

### *Learning Through Decisions.*

In designing security technologies, there is a tension between removing human decisions to automate security, and allowing the user the flexibility to make important choices [5]. The current version of Windows Update represents a compromise; most of the decisions about updates are made by the computer, removing the human from decision making. Many updates are downloaded and installed automatically, and Windows eventually automatically installs all downloaded updates even when they require a reboot. Some human decisions remain, particularly when they impact use of the computer, such as rebooting.

Removing the human from decisions, however, seems to have had an unintended side effect: users now find it difficult to understand what the computer is doing, and to correctly implement their part of the updates process. Having to make decisions as part of a security mechanism helps the user to learn how that mechanism works, what decisions are appropriate, and how to correctly execute those decisions. This learning may be direct, coming from feedback within the system. Or, this learning may be indirect learning, with the user seeking out the knowledge necessary to make better decisions.

Windows Updates has successfully automated so many security decisions that many users don't learn how to make intelligent security decisions about software updates. Instead, they struggle at understanding what their computer is doing, and often fail to execute even when they do make a decision.

This is important when some, but not all, security-relevant decisions can be automated. Removing the user from most of the decisions makes it more difficult for the user to intelligently make the remaining decisions that cannot be fully automated.

*Designing Update Systems.*

There is a fundamental tension here between learning and understanding what the computer is doing, and improving security by forcing the user to behave securely. It isn't clear which is a better strategy. Consider just the results in this paper: if usability were improved and users were able to accurately execute on their intentions, some users would end up less secure but many would end up more secure. The net effect on security isn't clear; it is possible that ignorance and inefficacy might be better for security than learning and usability.

There is also a tension here among the users. Some users want to trust the computer to make good decisions for them; that is, they want the computer to be its own system administrator. For these users, automating good decisions is valuable. However, other users want control over their computer, and rebel against the feeling of being forced into doing things they don't agree with (or just haven't thought about).

The software industry is currently struggling with these tensions. Windows update is clearly moving toward automating as much of the software update process as possible. A wide variety of other system applications are following. Firefox automatically downloads and installs updates with virtually no user intervention. Java is moving toward automatically installing updates, and Adobe is moving to a subscription model with automatically installed updates and upgrades. Apple's iOS 7 and OSX Mavericks now allow users to turn on a setting to automatically install updates to all software installed via the official App Stores.

However, some end-user "apps" and most business applications are moving to a much more explicit, user-driven update model. Some smartphones, for example, require the user to explicitly check for updates and choose to install them. Timing of this install is important. If you must pick a single install time, Windows did well. However, for any individual in a specific week, that time might not always be convenient. *Idle* on a computer does not necessarily mean *convenient* – it could be that users have important state that would be lost if an update was installed or the computer rebooted. A better strategy might be an adaptive mechanism that detects and when the user is finishing their work for the night and provides a notice at that time.

Almost all software on PCs eventually requires software updates, and many of these updates are security relevant. Each software vendor makes choices about how to distribute these updates. Our results suggest that automating updates similar to Windows Update or Firefox will lead to more uniform update installations, but will also result in many users not understanding what is happening on their computers and not being able to change things when they want to. On the other hand, manually installing updates may lead to better understanding about updates and greater feeling of control, but will also likely result in lower levels of security and compliance.

# 7. CONCLUSION

Quickly installing software updates is one of the best ways to protect your computer from malicious attackers. To improve security, companies such as Microsoft have moved to a model of automatic software updates that removes much of the decision-making by the end user. Using a combination of interviews, a survey, and log data, we compared what non-technical users understand about what their computer is doing to install software updates, what they want their computer to be doing, and what is actually happening on the computer.

We found that many end users had misunderstandings about what was happening on their computer; more than half our our subjects didn't correctly understand the automatic update settings on the computer, and more than half of our subjects did not understand when their updates were being installed. Furthermore, when users decided how they wanted to manage software updates, they often could not execute on that intention. This mismatch between intention and behavior frequently led to the computer being more secure, but also frequently led to the computer being less secure than intended.

# 8. ACKNOWLEDGMENTS

We thank Zack Girouard for his assistance with data collection and early analysis. We thank everyone associated with the BITLab at MSU for helpful discussions and feedback. This material is based upon work supported by the National Science Foundation under Grant No. CNS-1116544 and CNS-1115926.

# 9. REFERENCES

[1] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 41–46.

[2] BESNARD, D., AND ARIEF, B. Computer security impaired by legitimate users. *Computers & Security 23*, 3 (2004), 253–264.

[3] BILGE, L., AND DUMITRAS, T. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the ACM Conference on Computer and Communications Security* (New York, NY, USA, 2012), pp. 833–844.

[4] BREWER, D. D. Supplementary interviewing techniques to maximize output in free listing tasks. *Field Methods 14*, 1 (2002), 108–118.

[5] CRANOR, L. F. A framework for reasoning about the human in the loop. In *Usability, Psychology, and Security (UPSEC)* (2008).

[6] DILLMAN, D. A., SMYTH, J. D., AND CHRISTIAN, L. M. *Internet, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 3rd ed. Wiley, Hoboken, NJ, 2009.

[7] DOURISH, P., GRINTER, R. E., DELGADO DE LA FLOR, J., AND JOSEPH, M. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing 8*, 6 (2004), 391–401.

[8] EDWARDS, W. K., POOLE, E. S., AND STOLL, J. Security automation considered harmful? In *Proceedings of the New Security Paradigms Workshop, NSPW* (2007), pp. 33–42.

[9] FURNELL, S. Why users cannot use security. *Computers & Security 24*, 4 (June 2005), 274–279.

[10] GKANTSIDIS, C., KARAGIANNIS, T., AND VOJNOVIC, M. Planet scale software updates. In *ACM SIGCOMM Computer Communication Review* (New York, New York, USA, Aug. 2006), ACM, pp. 423–434.

[11] KAEMER, S., AND CARAYON, P. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. In *Applied Ergonomics* (2007), vol. 38, pp. 143–154.

[12] KAINDA, R., FLÉCHAIS, I., AND ROSCOE, A. W. Security and usability: Analysis and evaluation. In *International Conference on Availability, Reliability, and Security, ARES* (2010), IEEE, pp. 275–282.

[13] LAROSE, R., RIFON, N., LIU, S., AND LEE, D. Understanding online safety behavior: A multivariate model. In *The 55th Annual Conference of the International Communication Association* (New York City, 2005).

[14] LaRose, R., Rifon, N. J., and Enbody, R. Promoting personal responsibility for internet safety. *Communications of the ACM 51*, 3 (Mar. 2008), 71–76.

[15] Marconato, G., Nicomette, V., and Kaaniche, M. Security-related vulnerability life cycle analysis. In *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on* (2012), pp. 1–8.

[16] Microsoft. Microsoft Security Intelligence Report, Volume 13, January – June 2012.

[17] Miles, M. B., Huberman, A. M., and Saldaña, J. *Qualitative Data Analysis*. A Methods Sourcebook. SAGE Publications, Incorporated, Apr. 2013.

[18] Onwuegbuzie, A. J., and Leech, N. L. Validity and qualitative research: an oxymoron? *Quality & Quantity 41*, 2 (2007), 233–249.

[19] Symantec Corporation. Internet Security Threat Report, Volume 18, 2013.

[20] Thaler, R., and Sunstein, C. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, 2008.

[21] Vaniea, K., Rader, E., and Wash, R. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the ACM Conference on Human Factors in Computing (CHI)* (Toronto, Canada, 2014).

[22] von Ahn, L., Blum, M., Hopper, N. J., and Langford, J. CAPTCHA: Using hard ai problems for security. In *EUROCRYPT '03* (2003), pp. 294–311.

[23] Wash, R. Folk models of home computer security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2010).

[24] West, R. The Psychology of Security. *Communications of the ACM 51*, 4 (2008), 34–41.

[25] Wikipedia. Windows Update. `http://en.wikipedia.org/wiki/Windows_Update`; last retrieved September 17, 2013.

[26] Yee, K.-P. User interaction design for secure systems. In *International Conference on Information and Communications Security, ICICS* (2002), pp. 278–290.

[27] Zurko, M. E. User-Centered Security: Stepping Up to the Grand Challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (2005), IEEE, pp. 187–202.

# APPENDIX

## A. SURVEY QUESTIONS

**Q1**: Suppose there is a lottery where you have a 10% chance of winning $1000. What is the largest amount you would be willing to pay for a ticket in this lottery?

**Q2**: How do you see yourself: Are you in general a person who takes risk or do you try to evade risks? Please self-grade your choice (ranging between 0-10)

( ) 0 – not at all prepared to take risk
( ) 1
( ) 2
( ) 3
( ) 4
( ) 5
( ) 6
( ) 7
( ) 8
( ) 9
( ) 10 – very much prepared to take risks

**Q3**: How familiar are you with the following terms? Please rate your familiarity with each term below from None (no understanding) to Full (full understanding):

| | None | Little | Some | Good | Full |
|---|---|---|---|---|---|
| Security Update | ◯ | ◯ | ◯ | ◯ | ◯ |
| Critical Update | ◯ | ◯ | ◯ | ◯ | ◯ |
| Service Pack | ◯ | ◯ | ◯ | ◯ | ◯ |
| Software Update | ◯ | ◯ | ◯ | ◯ | ◯ |
| Optional Update | ◯ | ◯ | ◯ | ◯ | ◯ |
| Hotfix | ◯ | ◯ | ◯ | ◯ | ◯ |
| Upgrade | ◯ | ◯ | ◯ | ◯ | ◯ |

**Q4a**: Are you responsible for maintaining the laptop you brought with you today? Maintenance activities include things like installing and updating software, running antivirus, dealing with problems that may arise, etc.

( ) Yes
( ) No
( ) Other _____

**Q4b**: Is there another person (or people) who helps with maintaining the laptop you brought with you today?
*(Shown only if participant is responsible for maintaining their laptop.)*

( ) No, I do it by myself
( ) Yes, I share the responsibility with someone else
( ) Yes, I ask for help occasionally from someone who knows more than I do
( ) Other (please specify) _____

**Q5**: Please list the other people who use this computer, by their first name only. If nobody else uses this computer, leave the box blank:

**Q6**: Which of the following types of software do you have installed on the laptop you brought with you? Please check all that apply:

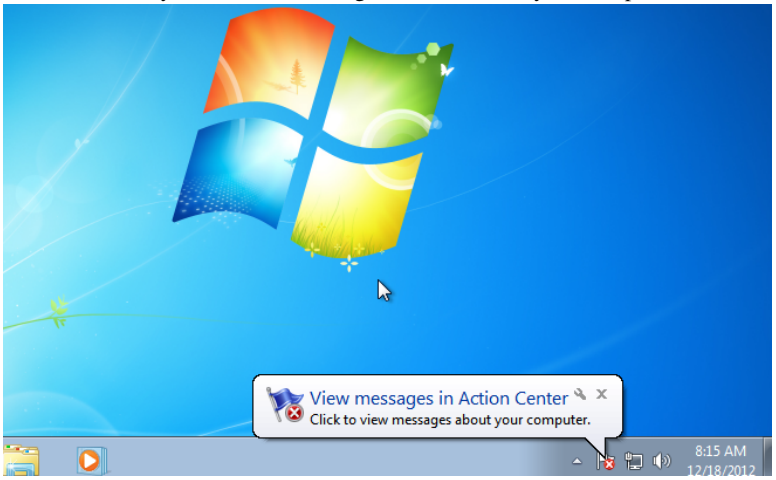
[ ] Windows operating system
[ ] Microsoft Office
[ ] Anti-virus software
[ ] Virus definitions or data files for your anti-virus software
[ ] Firewall software
[ ] Web browser, like Chrome or Firefox
[ ] Internet security software

[ ] Anti-spyware software
[ ] Adobe products, like Adobe Reader or Flash
[ ] Java
[ ] Database, like Oracle or Microsoft Access
[ ] Graphic design, like Photoshop
[ ] Multimedia, like iTunes, DVD player
[ ] Games
[ ] Communication, like Skype, Instant Message
[ ] Educational software

**Q7b**: Which of the following anti-virus programs do you have installed on your computer? Please check all that apply:
*Only shown if the participant claimed to have an anti-virus installed.*

[ ] Avast
[ ] AVG
[ ] Norton
[ ] McAfee
[ ] Microsoft
[ ] Kaspersky
[ ] I have an anti-virus program installed, but I don't remember which one
[ ] Other (please specify) _____

**Q8**: How often do you remember seeing a notification on your computer that looks similar to the following image?




( ) Never
( ) Rarely
( ) Sometimes
( ) Often
( ) Very Often

**Q9**: How long has it been since the last time any software on the laptop you brought with you was updated?

( ) Less than one month
( ) A couple of months
( ) 6 months or so
( ) About a year
( ) 1-2 years
( ) Longer than 2 years
( ) I don't know

**Q10**: In what ways do you remember finding out that a software update is available? Please check all that apply:

[ ] Checking the website of the software company

[ ] Checking for updates using the software itself

[ ] Email notification

[ ] News article

[ ] Mentioned by a friend or family member

[ ] Mentioned by a work colleague

[ ] Automated message on your computer

[ ] Other (please specify) _____

**Q11**:
Some kinds of software can check for software updates and let the user know when an update is available. Other kinds will check and then also download the update, so it is ready for the user to install. Still others automatically install software updates without any action by the user.
For each of the following kinds of software you indicated above that you have installed on the laptop you brought with you today, please indicate which kinds of software you remember behaving in the following ways:

CHECKING for updates automatically, and NOTIFYING you that new updates are available

CHECKING for and DOWNLOADING updates automatically, and NOTIFYING you that an update is ready to be installed

INSTALLING updates automatically, and NOTIFYING afterwards

INSTALLING updates automatically, WITHOUT notifying afterwards

If you aren't sure, choose your best guess.
*(Only software selected in Q6 was shown)*

| | Checking and Notifying | Checking, Downloading and Notifying | Installing and then Notifying | Installing Without Notifying |
|---|---|---|---|---|
| Windows operating system | [ ] | [ ] | [ ] | [ ] |
| Microsoft Office | [ ] | [ ] | [ ] | [ ] |
| Anti-virus software | [ ] | [ ] | [ ] | [ ] |
| Virus definitions or data files for your anti-virus software | [ ] | [ ] | [ ] | [ ] |
| Firewall software | [ ] | [ ] | [ ] | [ ] |
| Web browser, like Chrome or Firefox | [ ] | [ ] | [ ] | [ ] |
| Internet security software | [ ] | [ ] | [ ] | [ ] |
| Anti-spyware software | [ ] | [ ] | [ ] | [ ] |
| Adobe products, like Adobe Reader or Flash | [ ] | [ ] | [ ] | [ ] |
| Java | [ ] | [ ] | [ ] | [ ] |
| Database, like Oracle or Microsoft Access | [ ] | [ ] | [ ] | [ ] |
| Graphic design, like Photoshop | [ ] | [ ] | [ ] | [ ] |
| Multimedia, like iTunes, DVD player | [ ] | [ ] | [ ] | [ ] |
| Games | [ ] | [ ] | [ ] | [ ] |
| Communication, like Skype, Instant Message | [ ] | [ ] | [ ] | [ ] |
| Educational software | [ ] | [ ] | [ ] | [ ] |

**Q12**: Thinking about software installed on the laptop you brought with you that CHECKS for updates, NOTIFIES you that an update is ready, but does NOT automatically install it, how long after being notified do you typically install the update?
*(Only software selected in Q11 as Checking and Notifying was shown)*

| | Right Away | Later | Never |
|---|---|---|---|
| Windows operating system | ( ) | ( ) | ( ) |
| Microsoft Office | ( ) | ( ) | ( ) |
| Anti-virus software | ( ) | ( ) | ( ) |
| Virus definitions or data files for your anti-virus software | ( ) | ( ) | ( ) |
| Firewall software | ( ) | ( ) | ( ) |
| Web browser, like Chrome or Firefox | ( ) | ( ) | ( ) |
| Internet security software | ( ) | ( ) | ( ) |
| Anti-spyware software | ( ) | ( ) | ( ) |
| Adobe products, like Adobe Reader or Flash | ( ) | ( ) | ( ) |
| Java | ( ) | ( ) | ( ) |
| Database, like Oracle or Microsoft Access | ( ) | ( ) | ( ) |
| Graphic design, like Photoshop | ( ) | ( ) | ( ) |
| Multimedia, like iTunes, DVD player | ( ) | ( ) | ( ) |
| Games | ( ) | ( ) | ( ) |
| Communication, like Skype, Instant Message | ( ) | ( ) | ( ) |
| Educational software | ( ) | ( ) | ( ) |

**Q13**: Have you ever changed the settings for whether software automatically CHECKS for updates?

( ) Yes

( ) No

( ) I don't know

**Q14**: Have you ever changed the settings for whether software updates are INSTALLED automatically?

( ) Yes

( ) No

( ) I don't know

**Q15**: For each of the following types of software you have installed on the laptop you brought with you, how likely would you be to interrupt whatever task you were using the software for, to install a **security update**? Please rate how likely you would be to to do this from Very Unlikely to Very Likely:
*(Only software selected in Q6 was shown)*

| | Very Unlikely | Unlikely | Undecided | Likely | Very Likely |
|---|---|---|---|---|---|
| Windows operating system | ( ) | ( ) | ( ) | ( ) | ( ) |
| Microsoft Office | ( ) | ( ) | ( ) | ( ) | ( ) |
| Anti-virus software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Virus definitions or data files for your anti-virus software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Firewall software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Web browser, like Chrome or Firefox | ( ) | ( ) | ( ) | ( ) | ( ) |
| Internet security software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Anti-spyware software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Adobe products, like Adobe Reader or Flash | ( ) | ( ) | ( ) | ( ) | ( ) |
| Java | ( ) | ( ) | ( ) | ( ) | ( ) |
| Database, like Oracle or Microsoft Access | ( ) | ( ) | ( ) | ( ) | ( ) |
| Graphic design, like Photoshop | ( ) | ( ) | ( ) | ( ) | ( ) |
| Multimedia, like iTunes, DVD player | ( ) | ( ) | ( ) | ( ) | ( ) |
| Games | ( ) | ( ) | ( ) | ( ) | ( ) |
| Communication, like Skype, Instant Message | ( ) | ( ) | ( ) | ( ) | ( ) |
| Educational software | ( ) | ( ) | ( ) | ( ) | ( ) |

**Q16**: For each of the following types of software you have installed on the laptop you brought with you, how willing would you be to interrupt whatever task you were using the software for, to install **OTHER, NON-security updates**? Please rate how likely you would be to to do this from Very Unlikely to Very Likely:
*(Only software selected in Q6 was shown)*

| | Very Unlikely | Unlikely | Undecided | Likely | Very Likely |
|---|---|---|---|---|---|
| Windows operating system | ( ) | ( ) | ( ) | ( ) | ( ) |
| Microsoft Office | ( ) | ( ) | ( ) | ( ) | ( ) |
| Anti-virus software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Virus definitions or data files for your anti-virus software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Firewall software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Web browser, like Chrome or Firefox | ( ) | ( ) | ( ) | ( ) | ( ) |
| Internet security software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Anti-spyware software | ( ) | ( ) | ( ) | ( ) | ( ) |
| Adobe products, like Adobe Reader or Flash | ( ) | ( ) | ( ) | ( ) | ( ) |
| Java | ( ) | ( ) | ( ) | ( ) | ( ) |
| Database, like Oracle or Microsoft Access | ( ) | ( ) | ( ) | ( ) | ( ) |
| Graphic design, like Photoshop | ( ) | ( ) | ( ) | ( ) | ( ) |
| Multimedia, like iTunes, DVD player | ( ) | ( ) | ( ) | ( ) | ( ) |
| Games | ( ) | ( ) | ( ) | ( ) | ( ) |
| Communication, like Skype, Instant Message | ( ) | ( ) | ( ) | ( ) | ( ) |
| Educational software | ( ) | ( ) | ( ) | ( ) | ( ) |

**Q17**: Which of these statements do you agree with the most? Please drag-and-drop the statements below to rank them according to your level of agreement with each statement, from (1) Most Agreement to (5) Least Agreement:

1. Installing a software update repairs software (e.g., fixes bugs or malfunctions) and makes my computer more reliable.
2. Installing a software update improves software so that it works better and can do new things.
3. Installing a software update protects software so that it is less vulnerable.
4. Installing a software update is routine maintenance that keeps my computer in good working order.
5. Installing a software update keeps my computer "up to date" so it doesn't fall behind or become obsolete as quickly.

**Q18**: Was it difficult for you to rank the statements?

( ) No

( ) Yes (Please explain) _____

**Q19**: How often have you experienced an update that caused your computer to stop working properly?

( ) Never

( ) Rarely

( ) Sometimes

( ) Often

( ) Very Often

**Q20**: How worried are you about updates causing your computer to stop working properly?

( ) Never thought about this before

( ) Not worried

( ) Slightly worried

( ) Worried

( ) Very worried

**Q21**: Have you ever had one of the following experiences? Please check all that apply:

[ ] Received a phishing message or other scam email

[ ] Warning in a web browser that says, "This site may harm your computer?"

[ ] Unwanted popup windows

[ ] Computer had a virus

[ ] Someone broke in or "hacked" the computer

[ ] Stranger used your credit card without your knowledge or permission

[ ] Identity theft more serious than use of your credit card number without permission

**Q22**: How familiar are you with the following Internet-related terms? Please rate your familiarity with each term below from None (no understanding) to Full (full understanding):

| | None | Little | Some | Good | Full |
|---|---|---|---|---|---|
| RSS | ( ) | ( ) | ( ) | ( ) | ( ) |
| Reload | ( ) | ( ) | ( ) | ( ) | ( ) |
| Widget | ( ) | ( ) | ( ) | ( ) | ( ) |
| Spyware | ( ) | ( ) | ( ) | ( ) | ( ) |
| Proxypod | ( ) | ( ) | ( ) | ( ) | ( ) |
| Tagging | ( ) | ( ) | ( ) | ( ) | ( ) |
| Cache | ( ) | ( ) | ( ) | ( ) | ( ) |
| Frames | ( ) | ( ) | ( ) | ( ) | ( ) |
| Newsgroup | ( ) | ( ) | ( ) | ( ) | ( ) |
| PDF | ( ) | ( ) | ( ) | ( ) | ( ) |
| Torrent | ( ) | ( ) | ( ) | ( ) | ( ) |
| Malware | ( ) | ( ) | ( ) | ( ) | ( ) |
| Wiki | ( ) | ( ) | ( ) | ( ) | ( ) |
| Podcasting | ( ) | ( ) | ( ) | ( ) | ( ) |
| Favorites | ( ) | ( ) | ( ) | ( ) | ( ) |
| Blog | ( ) | ( ) | ( ) | ( ) | ( ) |

**Q23**: Have you ever worked in a "high tech" job such as computer programming, IT, or computer networking?

( ) Yes

( ) No

( ) Other (please specify) _____

**Q24**: How old are you? Please type your answer here: _____

**Q25**: What is the last grade or class you completed in school?

( ) None, or grades 1-8

( ) High school incomplete (grades 9-11)

( ) High school graduate (grade 12 or GED certificate)

( ) Technical, trade or vocational school AFTER high school

( ) Some college, no 4-year degree (includes associate degree)

( ) College graduate (B.S., B.A., or other 4-year degree)

( ) Post-graduate training/professional school after college (toward a Masters/Ph.D., Law or Medical school)

( ) Post-graduate degree (Masters/Ph.D., Law or Medical school)

( ) I don't know

( ) Other (please specify) _____

**Q26**: What is your gender?

( ) Man

( ) Woman

( ) Prefer not to answer

**Q26**: What is your race?

( ) American Indian or Alaska Native

( ) Asian or Pacific Islander

( ) Black or African-American

( ) Hispanic or Latino

( ) White

( ) Other (please specify) _____